Listing of the Claims:

The listing of the claims below replaces all previous listings of the claims.

1. (Currently Amended) A ~~storage system comprising: a~~ removable storage device configured to communicate ~~communication~~ with a host device over a universal serial bus (USB), the removable storage device comprising:

a flash memory for storing at least one permission for determining access to the flash memory;

a biometric interface for receiving, independently of the host device, a request to access the flash memory at the removable storage device;

a processor for managing access to the flash memory, independently of the host device, based on a comparison of the ~~comparing said~~ request to the ~~said~~ at least one permission, the comparison being independent, requiring no management by an operating system of the host device, such that if the ~~said~~ at least one permission includes a particular access type that matches the access requested in the ~~said~~ request, the processor provides such access to the flash memory, ~~is provided,~~ and alternatively if the ~~said~~ at least one permission does not include a particular access type that matches the access requested in the ~~said~~ request, the processor denies such access to the flash memory; ~~is denied;~~ and

a USB interface controller for communicating with the USB bus of the host device and, if permitted, for transmitting data from the ~~said~~ processor.

2. (Cancelled).

3. (Cancelled).

4. (Previously Presented) The storage system of claim 1, wherein said biometric interface comprises:

a sample collector for collecting a biological parameter of a user.

5. (Cancelled).

6. (Previously Presented) The storage system of claim 4, wherein said biological parameter of the user is a fingerprint of the user.

7. (Previously Presented) The storage system of claim 1, further comprising:

a RAM component for storing data for performing said at least one instruction of said data processor.

8. (Previously Presented) The storage system of claim 1, further comprising:

a cryptographic chip for encrypting and decrypting data.

9. (Previously Presented) The storage system of claim 8, wherein said cryptographic chip performs an authentication process.

10. (Previously Presented) The storage system of claim 8, wherein said cryptographic chip emulates a smart card.

11. (Previously Presented) The storage system of claim 10, wherein said cryptographic chip stores encrypted smart card data.

12. (Previously Presented) The storage system of claim 8, wherein said cryptographic chip performs encryption immediately upon receiving a command from said processor.

13. (Previously Presented) The storage system of claim 12, wherein said cryptographic chip creates a cryptographic signature with a hash immediately upon receiving a command from said processor.

14. (Previously Presented) The storage system of claim 8, wherein said cryptographic chip further comprises a cryptographic chip memory for storing at least one cryptographic key and at least one cryptographic instruction for encrypting and decrypting data, such that said cryptographic chip forms a removable encryption engine.

15. (Previously Presented) The storage system of claim 14, wherein said encrypted data is stored on said cryptographic chip memory.

16. (Previously Presented) The storage system of claim 15, wherein said cryptographic chip memory is a separate flash memory device from said flash memory device.

17. (Previously Presented) The storage system of claim 15, wherein said cryptographic chip memory is said flash memory device.

18-50. (Canceled).

51. (New) A method for determining whether to provide access to a flash memory, the method comprising:

receiving a request to access a flash memory at a biometric interface of an access control module, independent of a host device, the access control module configured to communicate with the host device over a universal serial bus (USB); and

managing access to the flash memory with a processor of the access control device, independent of the host device, based on a comparison of the request to at least one permission for determining access to the flash memory, the comparison being independent of, and requiring no management by, an operating system of the host device;

wherein managing access to the flash memory comprises:

providing, with a processor of the access control module, access to the flash memory in response to determining that the at least one permission

includes a particular access type that matches the access requested in the request; and

denying, with a processor of the access control module, access to the flash memory in response to determining that the at least one permission does not include a particular access type that matches the access requested in the request.

52. (New) The method of claim 51, wherein a removable storage device comprises the access control module and the flash memory.

53. (New) The method of claim 51, wherein the access control module is distinct from a removable storage device comprising the flash memory.

54. (New) An access control device configured to communicate with a host device over a universal serial bus (USB), the access control device comprising:

a biometric interface for receiving, independent of the host system, a request at the access control device to access a flash memory; and

a processor for managing access to the flash memory independent of the host device based on a comparison of the request to at least one permission, the comparison being independent of, and requiring no management by an operating system of the host device, such that if the at least one permission includes a particular access type that matches the access requested in the request, the processor provides such access to the flash memory, and alternatively if the at least one permission does not include a particular access type that matches the access requested in the request, the processor denies such access to the flash memory.